Lattice-Based Cryptography

Lattices

NP-Hard Problems in Lattices (SIS, SVP, etc)

Kübra SEYHAN Sedat AKLEYLEK

Department of Computer Engineering,
Cyber Security and Information Technologies Research and Development,
Ondokuz Mayıs University, Samsun, Turkey

September 8, 2022

Intermediate and Advanced Course on Post-Quantum Cryptography

Baku, Azerbaijan

This work was partially supported by TUBITAK under grant no. 121R006.

Outline

- Public-Key Cryptography
- Post-Quantum Cryptography
- Basic Definitions
- NP-Hard Problems in Lattices
- Parameter Estimation for Lattice Problems
- Conclusion